WHAT IS CLAIMED IS:

1. A method for encrypting data in an access virtual private network (VPN), comprising the steps of:

performing a link control protocol (LCP) negotiation regarding at least one of an authentication method, data compression, maximum data size receivable, link status monitoring, and whether to perform data encryption;

checking a user identification (ID) and a password when the LCP negotiation determines that mutual authentication is required, said negotiation being conducted by two terminals according to an LCP negotiation condition at the step of performing the LCP negotiation;

performing data encryption when the step of performing the LCP negotiation results in a determination that data encryption is to be performed;

performing network control protocol (NCP) negotiation in order to negotiate information for a Layer 3 communication access between a user and a private network; and

transmitting and receiving data by forming a session between the user and the private network when the NCP negotiation is performed between the user and the private network.

2. The method according to claim 1, wherein the NCP negotiation is performed after the data encryption is performed.

3. The method according to claim 1, wherein the NCP negotiation is performed when it is determined, during performance of the LCP negotiation, that authentication and data encryption are not required.

4. The method according to claim 1, wherein an item for selecting whether to perform data encryption is added to an LCP negotiation option table of the user and the private network in advance of the step of performing the LCP negotiation.

5. The method according to claim 1, wherein the step of checking the user ID and the password comprises using a password authentication protocol (PAP) for providing user authentication by delivering the user ID and the password in form of a text.

6. The method according to claim 1, wherein the step of checking the user ID and the password comprises using a challenge handshake authentication protocol (CHAP) for providing user authentication using a hash function.

7. The method according to claim 1, wherein the step of performing data encryption comprises using a data encryption standard (DES).

8. The method according to claim 1, wherein the step of performing data encryption comprises using a user password as a key value for encryption.

9. The method according to claim 1, wherein the LCP negotiation is performed with respect to both the authentication method and whether to perform data encryption.

10. The method according to claim 9, wherein the step of performing data encryption comprises using a user password as a key value for encryption.